Publication No.: 10-2001-0114188
Applicant: TERUTEN INC.

ABSTRACT

The present invention aims to provide a system and method not only for processing digital data provided in a stream manner but also for protecting decoded content data from being reproduced and distributed without permission, and a storage medium that implements the method in a software manner. In order to achieve the above-described object, the stream data protection system of the present invention includes a control means for providing information about stream data to be requested for execution and identification information about execution programs capable of executing the stream data, a filtering means for storing the identification information about the execution programs, determining whether identification information about a certain execution program has been stored in the control means when the certain execution program requests the stream data for execution, and determining the request to be effective and passing the request therethrough if the identification information about the execution program has been stored in the control means, and a stream data supply means for requesting stream data based on the provided information about the stream data when the stream data request passed through the filtering means is received, and providing the stream data to the execution program when the requested data are supplied.

(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(51) 。Int. Cl. [7]
H04L 9/18

(11) 공개번호 특2001-0114188
(43) 공개일자 2001년12월29일

(21) 출원번호 10-2001-0050151
(22) 출원일자 2001년08월21일

(71) 출원인 (주)테르텐
윤석구
서울특별시 강남구 대치동 901-66번지

(72) 발명자 김성엽
서울특별시광진구군자동372-2
이새록
서울특별시광진구자양3동우성2차아파트202-1208
윤석구
경기도안양시동안구범계동목련우성아파트505-1703
이영
경기도안양시동안구범계동목련우성아파트505-1703

(74) 대리인 박현철

심사청구 : 있음

(54) 스트림 방식으로 실행되는 디지털 데이터의 보호를 위한시스템 및 그 방법

요약

본 발명은 스트림 방식으로 제공되는 디지털 데이터를 처리할 수 있으면서, 동시에 암호가 풀린 컨텐츠 데이터를 무단 복제나 배포로부터 보호할 수 있는 시스템 및 그 방법과 이를 소프트웨어적으로 구현한 프로그램 저장 매체를 제공하고자 하는 것이다. 상기와 같은 목적을 달성하기 위한 본 발명의 스트림 데이터 보호 시스템은, 실행하고자 요청된 스트림 데이터의 정보 및 이 스트림 데이터를 실행할 수 있는 실행 프로그램의 식별 정보를 제공하는 제어 수단과, 상기 제공된 실행 프로그램의 식별 정보를 저장하고, 소정의 실행 프로그램이 상기 스트림 데이터를 실행하고자 요청하는 경우에 상기 소정의 실행 프로그램의 식별 정보가 상기 접근 제어 수단에 저장되었는지를 판단하고, 상기 소정의 실행 프로그램의 식별 정보가 저장되었다고 판단되면 상기 실행 요청을 유효한 것으로서 통과시키는 필터링 수단과, 상기 필터링 수단을 통과한 스트림 데이터 요청을 입력받으면, 상기 제공된 스트림 데이터의 정보를 바탕으로 스트림 데이터를 요청하고, 요청된 스트림 데이터를 공급받으면 상기 스트림 데이터를 요청한 실행 프로그램에 제공하는 스트림 데이터 공급 수단을 포함하여 구성된다.

대표도
도 1

명세서

도면의 간단한 설명

도 1은 본 발명의 기본적인 실시예를 나타내는 모식도.

도 2는 단일의 스트림 공급 수단을 구비한 본 발명의 또 다른 실시예를 나타내는 모식도.

도 3은 암호화된 스트림 데이터를 복호화하는 복호화 수단을 추가로 구비한 본 발명의 또 다른 실시예를 나타내는 모식도.

도 4는 네트워크로 연결된 저장 장치 및 외부 스트림 공급 수단을 구비한 본 발명의 또 다른 실시예를 나타내는 모식도.

도 5는 스트림 데이터에 관한 정보를 외부 스트림 공급 수단에 제공하는 본 발명의 또 다른 실시예를 나타내는 모식도.

도 6은 외부 스트림 공급 수단이 동적 라이브러리 형태로 구성된 본 발명의 또 다른 실시예를 나타내는 모식도.

도 7은 버퍼링 수단을 추가한 본 발명의 또 다른 실시예를 나타내는 모식도.

도 8은 버퍼링 수단을 전후한 암호화 및 복호화 수단을 추가로 구비한 본 발명의 또 다른 실시예를 나타내는 모식도.

< 도면의 주요 부분에 대한 설명>

110: 제어기 120: 필터링 수단

130: 등록된 실행 프로그램 140: 등록되지 않은 실행 프로그램

150: 내부 스트림 공급 수단 160: 외부 스트림 데이터 공급 수단

200: 파일 시스템 영역

발명의 상세한 설명

발명의 목적

발명이 속하는 기술 및 그 분야의 종래기술

본 발명은 네트워크 또는 클라이언트 시스템의 저장 장치에서 스트리밍 방식으로 제공되는 디지털 데이터를 사용하는 컴퓨터 시스템 및 그 방법과 프로그램 매체에 관한 것으로, 좀 더 상세하게는 스트리밍 디지털 데이터의 보호 기술에 관한 것이다.

최근 인터넷 등 온라인을 통해 디지털 컨텐츠 데이터의 유통이 일반화되고 있다. 디지털 컨텐츠란 일반적으로 우리가 알고 있는 전통적인 문학 작품, 그림, 영화, 음악 및 게임 등에 더하여 시장 조사 자료, 온라인 교육 내용, 경제적으로 유용한 데이터베이스 등, 시장이나 소비자가 필요로 하는 모든 정보를 포함하는 개념이다.

이러한 디지털 컨텐츠는 대부분 많은 노력을 들여 창조되거나 개발된 것이므로 저작권자 입장에서는 법적, 기술적으로 이를 보호할 수 있는 보안 기술이 절실한 것이며, 이러한 사회적 욕구에 부응하여 다양한 암호화 방법 및 인증 방법이 개발되어 왔다.

최근의 디지털 컨텐츠의 이용은 좀 더 복잡한 보안기술을 요구하고 있다. 즉, 원천적으로 무단 사용을 하는 것이 아니라, 일단 최초 이용은 유료로 다운로드 등을 받아 권한을 가진 사용을 하게 되지만, 이를 하드 디스크 등의 저장 장치에 무단으로 보관한 후, 보관된 파일을 복제하거나 배포하는 2차적 행위에서 저작권자의 권리를 침해하는 양상이 바로 그것이다. 이 경우, 처음의 유효한 사용과 그 이후의 불법적인 사용을 구분해서 제어해야 하는 복잡함이 발생한다.

최근 관심이 고조되고 있는 디지털 컨텐츠 불법 복제 방지 기술인 DRM(Digital Rights Management)은 이러한 문제를 해결할 하나의 대안으로 인식되고 있다.

DRM 기능을 간단히 설명하면, 암호화된 컨텐츠가 실행되기 위해서는 역시 복호화가 반드시 필요하지만, 기존의 방법과는 달리 DRM 제어기가 실행 프로그램 내부 또는 이에 연계하여 존재하므로 복호화된 데이터가 이 영역의 외부로 나가서 저장될 필요없이 바로 그 내부에 함께 존재하는 실행 프로그램으로 전달되어 실행되도록 구성되어 있으므로, 사용자가 이 영역 내부에서만 처리되는 복호화된 컨텐츠에 허가받지 않은 접근 행위를 할 수 없는 것이다. 따라서, 사용자는 무단 복제 및 배포 행위를 할 수 없게 된다.

이 기술의 문제점은 DRM 제어기를 개발하는 개발사에 따라 그 암호화 및 복호화 방법이 수 없이 다양하다는 것이다. 따라서, 하나의 실행 프로그램이 실행해야 할 컨텐츠 데이터도 다양한 DRM에 의해 복호화된 데이터 일 것이므로, 결국 이 실행 프로그램은 이 다양한 DRM 제어기를 모두 내장해야 한다는 문제점이 발생한다. 이것은 현실적으로 불가능한 일이다. 따라서, 이 방법은 임시적인 방법일 뿐 아니라 이 방법 자체가 또 다른 컨텐츠 유통의 장애물로 등장할 수 있다.

본원 발명의 출원인에 의해 2001. 6. 25에 출원된 " 디지털 데이터의 안전한 전달 및 실행을 위한 보안 시스템" (출원번호: 2001-34583)에서는 이러한 종래 DRM 제어기의 문제점을 해결한 간단하면서도 획기적인 발명이 제시되어 있다.

상기 출원에서는, 암호가 풀린 컨텐츠 데이터 파일을 특정 저장 영역에 존재시킨 후, 이 지정 영역의 파일을 실행시킬 수 있는 실행 프로그램을 사전에 등록하고 이 실행 프로그램의 호출에 대해서만 데이터 파일이 실행될 수 있도록 구성함으로써, 실행 가능한 실행 프로그램을 제한하면서, 동시에 DRM 제어기와는 별개로 존재토록 구성한 점에 그 특징이 있다.

최근 컨텐츠 데이터 파일은 그 크기가 600 MB 이상을 차지하는 것들도 있는데, 이 정도의 크기를 가진 데이터 파일을 실행시키기 위해서는 스트림 방식이 필수적이다. 스트림 방식이란 선행 데이터 일부가 실행 프로그램에서 실행되는 동안, 후속 데이터들이 일정 단위로 램 메모리에 올려져 다음 실행을 대기하는 방식으로 실행 및 로딩을 동시에 수행할 수 있으며, 또한 미분화된 데이터 파일 조각들을 처리함으로써 파일 전체를 핸들링하는 기존 방법에 대비해서 대단히 속도가 빠르고 효율적이다.

하지만, 컨텐츠 데이터가 암호화된 파일일 경우, 이것을 스트림 방식으로 실행시키기 위해서는 암호화된 스트림 데이터 조각을 데이터 조각마다 복호화해서 실행시켜야 하며, 특히 전술한 DRM 방식으로 암호화된 경우 매 실행 프로그램마다 복수 개의 DRM제어기가 필요하게 된다. 또한, 기존의 스트림 방식은 복호화된 상태에서 데이터를 해킹당할 수 있으므로 이에 대한 대비책도 요구되어 왔다.

본 발명은 상기 " 디지털 데이터의 안전한 전달 및 실행을 위한 보안 시스템" 발명의 구성상 특징을 스트림 데이터의 보호 방식에 응용한 것으로서, 스트림 방식으로 전송되거나 복호화되는 컨텐츠 데이터를 사용자가 임의로 복제하거나 배포하지 못하도록 구성하면서, 동시에 특정 DRM제어기에 구애받지 않는 새로운 스트림 데이터 보호 시스템 및 그 방법에 관한 발명이다.

발명이 이루고자 하는 기술적 과제

본 발명은 스트림 방식으로 제공되는 디지털 데이터를 처리할 수 있으면서, 동시에 암호가 풀린 컨텐츠 데이터를 무단 복제나 배포로부터 보호할 수 있는 시스템 및 그 방법과 이를 소프트웨어적으로 구현한 프로그램 저장 매체를 제공하고자 하는 것이다.

본 발명의 또 다른 목적은 상기와 같은 구성을 통하여 컨텐츠 데이터의 스트림 처리를 좀 더 안전하고 원할하게 수행토록 하는 시스템 및 방법을 제공하는 것이다.

발명의 구성 및 작용

상기와 같은 목적을 달성하기 위한 본 발명의 스트림 데이터 보호 시스템은, 실행하고자 요청된 스트림 데이터의 정보 및 이 스트림 데이터를 실행할 수 있는 실행 프로그램의 식별 정보를 제공하는 제어 수단과, 상기 제공된 실행 프로그램의 식별 정보를 저장하고, 소정의 실행 프로그램이 상기 스트림 데이터를 실행하고자 요청하는 경우에 상기 소정의 실행 프로그램의 식별 정보가 상기 접근 제어 수단에 저장되었는지를 판단하고, 상기 소정의 실행 프로그램의 식별 정보가 저장되었다고 판단되면 상기 실행 요청을 유효한 것으로서 통과시키는 필터링 수단과, 상기 필터링 수단을 통과한 스트림 데이터 요청을 입력받으면, 상기 제공된 스트림 데이터의 정보를 바탕으로 스트림 데이터를 요청하고, 요청된 스트림 데이터를 공급받으면 상기 스트림 데이터를 요청한 실행 프로그램에 제공하는 스트림 데이터 공급 수단을 포함하여 구성된다. 또한, 상기 스트림 데이터를 저장하고 있으면서, 상기 스트림 공급 수단으로부터의 요청에 응답하여 저장된 스트림 데이터를 상기 스트림 공급 수단으로 제공하는 스트림 데이터 저장 수단을 더 포함할 수 있다.

상기 스트림 데이터 공급 수단은, 반드시 상기 필터링 수단을 통해서 실행 프로그램과의 데이터 통신을 수행하는 제1 스트림 공급 수단과, 상기 스트림 데이터 저장 수단으로부터 스트림 데이터를 공급받아 상기 필터링 수단을 통하지 않고 상기 제1 스트림 공급 수단과 데이터 통신을 수행하는 제2 스트림 공급 수단을 포함할 수 있는데, 상기 요청된 스트림 데이터가 암호화된 데이터일 경우에는 상기 제2 스트림 공급 수단이 스트림 데이터를 복호화하여 상기 스트림 데이터 공급 수단으로 제공하는 복호화 수단을 내부에 포함할 수 있다. 또한, 이 복호화 수단은 상기 제2 스트림 공급 수단과는 별개로 존재할 수도 있다.상기 제2 스트림 공급 수단은 상기 제1 스트림 공급 수단의 라이브러리거나 또는 독립적으로 실행될 수 있는 모듈일 수 있으며, 두 스트림 공급 수단은 네트워크로 연결된 것도 가능하다.

이하, 도면의 실시예들을 참조하여 본 발명을 상세히 설명한다.

도 1은 본 발명의 일 실시예의 구성을 나타내는 모식도이다. 도 1에 도시된 실시예는 클라이언트 시스템, 가령 사용자의 PC에 로컬로 암호화되어 저장된 컨텐츠 데이터를 스트림 방식으로 복호화하여 실행시키는 실시예를 보여주고 있다. 도 1에서는, 클라이언트 시스템 내부에서 필터링 수단(120)에 의해 데이터들의 저장 및 출력을 제어받는 파일 시스템 영역(200)과, 파일 시스템(200)의 최상부에서 파일 시스템 영역(200)내의 모든 데이터의 입출력을 제어하고 데이터 실행 명령의 유효 여부를 판단하는 필터링 수단(120)과, 역시 파일 시스템 영역(200)내에서 외부에 스트림 데이터를 요청하고 전송되어 온 스트림 데이터가 상기 필터링 수단(120)을 통과하여 실행 프로그램(130)으로 전송되도록 처리하는 파일 시스템 내부의 스트림 공급 수단(150)과, 상기 필터링 수단(120)에 접근 제어 리스트로서 특정 실행 프로그램을 등록하고, 동시에 실행되어야 할 데이터 파일 및 외부 스트림 데이터 공급 수단(160)에 관한 정보를 제공하는 제어기(110)와, 저장 장치(170)로부터 암호화된 컨텐츠 데이터를 전송받아 이를 복호화하고 상기 내부 스트림 공급 수단(150)의 데이터 요청에 대한 응답으로 이 복호화된 데이터를 제공하는 파일 시스템 외부의 스트림 공급 수단(160)과, 데이터 파일을 실행할 수 있는 실행 프로그램(130)과, 필터링 수단에 등록되지 않아서 데이터 파일을 실행할 수 없는 실행 프로그램(140)이 한 예로 도시되어 있다.

먼저, 컨텐츠 데이터를 실행하고자 하는 사용자는 탐색기나 인터넷 브라우저(도시되지 않음) 등을 이용하여 실행하고

자 하는 컨텐츠 데이터 파일을 선택한다. 컨텐츠 데이터 파일의 실행 명령이 접수되면, 제어기(110)는 사용 정책 등을 체크하여 이 실행 명령이 유효한 명령인지를 파악한다. 사용 정책이란 컨텐츠 데이터 사용자와 컨텐츠 데이터 공급자간에 맺어진 계약에 근거하여 상기 실행 명령이 유효한 행위인지를 판단하는데 사용되는 것을 의미한다. 가령, 사용자의 ID등을 입력받으면 이를 통해 사용자가 누구인지를 인지하고 해당 사용자가 상기 컨텐츠 데이터를 현재 이용할 수 있는 권한을 갖고 있는가를 상기 사용 정책을 바탕으로 판단하는 것이다. 이러한 사용 정책의 체크는 온라인으로 데이터 공급자 측의 서버와 제어기(110)간에 실시간 통신으로 체크하거나, 또는 사용자의 클라이언트 시스템에 내장된 모듈로 체크하여 제어기에 통보하는 방식 등을 이용할 수 있다. 이러한 기능은 반드시 제어기(110)가 수행할 필요는 없으며, 제어기가 다른 모듈이나 네트워크로부터 유효성을 판단한 정보를 입력받아 다음 프로세스를 진행할 수도 있다.

상기 사용 정책을 바탕으로 실행 명령이 권한 있는 유효한 명령이라고 판단되면, 제어기(110)는 선택된 컨텐츠 데이터를 실행할 수 있는 실행 프로그램(130)을 선정하여 이 실행 프로그램의 식별 정보, 가령 프로세스 ID 등을 필터링 수단(120)에 등록시킨다(S1). 도 1에서는 이를 간단히 모식화하여 실행 프로그램 A.exe(130)가 컨텐츠 데이터인 C.avi를 실행할 수 있는 실행 프로그램으로서 필터링 수단(120)에 등록된 상태를 보여주고 있다. 이 등록 정보는 향후 파일 시스템 영역(200)에 대한 접근 제어 리스크로 사용되어, 등록된 실행 프로그램(130)의 호출 명령만이 유효한 것으로 처리하는데 사용된다. 이와 관련한 상세한 사항들은 상기 출원 제 2001-34583호에 기술된 바와 동일하거나 유사하다.

상기 단계(S1)를 전후하여 제어기(110)는 실행되어야 할 컨텐츠 데이터 파일(도 1에서 C.avi)의 식별 정보와, 그 데이터의 존재 위치를 나타내는 경로 및 외부에서 스트림 데이터를 공급해 주어야 할 외부 스트림 공급 수단에 관한 정보를 파일 시스템 영역(200)에 등록시킨다(S1'). 파일 시스템 영역에 등록시키는 실시예로는 상기 필터링 수단(120) 내부에 등록시키거나, 내부 스트림 데이터 공급 수단(150)의 내부에 등록시키는 것 및 파일 시스템 영역(200) 내부에 존재하면서 필터링 수단(120) 및 내부 스트림 공급 수단(150)과 연결되어 상기 정보들을 제공할 수 있는 제3의 모듈(160)에 등록시키는 등의 어떠한 상황도 모두 포함된다.

상기 등록해야 할 각 정보 중에서 외부 스트림 공급 수단(160)에 관한 정보란, 어디에 있는 어떤 외부 스트림 공급 수단을 사용할 것인가에 관한 정보이다. 이것이 필요한 이유는, 내부 스트림 공급 수단(150)이 외부 스트림 공급 수단에 데이터를 요청할 때에 어느 외부 스트림 공급 수단에 데이터를 요청해야 할지를 알아야 하기 때문이다. 도 1에서는 예시적으로 그 공급 수단이 C:\B.exe라고 가정한 다음, 이를 파일 시스템 내부(200)에 등록하여 내부 스트림 공급 수단(150)에 통지하는 상황을 나타내고 있다. 이 경우, 내부 스트림 공급 수단(150)은 자신이 위치한 클라이언트 시스템의 저장 영역 C에서 B.exe라는 프로그램을 실행시켜 데이터를 전송하도록 명령하게 된다. 여기서 외부란 필터링 수단(120)에 의해 데이터 입출력이 제한되고 통제되는 특정 영역인 파일 시스템(200)의 바깥을 의미한다. 따라서 내부란, 그 역으로 필터링 수단(120)에 의해 데이터 입출력이 제한되고 통제되는 파일 시스템 영역(200)을 의미하게 된다.

외부 스트림 공급 수단에 관한 정보로는 이 밖에도 URL개념이 포함될 수 있는데, 가령 www.m.com/B.exe라는 방식으로 되어 있으면 내부 스트림 공급 수단(150)이 인터넷 연결 도구(도시하지 않음)를 통해 www.m.com이라는 사이트에 접속하고, 이 영역에 존재하는 B.exe를 이용하여 스트림 데이터를 전송하라는 명령이 된다. 외부 스트림 공급 수단은 이 외에도 DLL(Dynamic link library) 등이 가능한데, 이에 대한 상세한 사항은 후술한다.

상기 내부 스트림 공급 수단(150)에 등록해야 할 정보 중에는 실행되어야 할 컨텐츠 데이터에 관한 정보가 제공되어야 한다. 이것은 내부 스트림 공급 수단(150)이 어느 데이터를 요청하는지를 외부 스트림 공급 수단(160)에 알려 주기 위해서 필요한데, 이 정보에는 파일 이름 및 그 경로가 포함될 수 있다. 도 1에서는 한 예로 클라이언트 시스템의 저장 영역 C의 work라는 폴더에 저장된 경우인 "C:\work\C.avi"를 컨텐츠 데이터 정보로 제공하고 있다.

또한, 상기 컨텐츠 데이터에 관한 정보가 제공될 때, 이를 실행할 수 있도록 상기 필터링 수단(120)에 등록된 실행 프로그램(130)의 정보가 매칭되어 제공되어야 한다. 이것은 필터링 수단에 등록(S1)시키는 작업에 의해 배치(batch) 프로세스로 등록되거나, 또는 도시된 바와 같이 따로 제공(S1')될 수 있다. 실행 프로그램 정보가 컨텐츠 데이터 정보와 매칭되어 제공되어야 하는 이유는, 이 매칭된 정보를 통해 실행 프로그램(130)의 호출에 대해 어느 데이터를 제공해야 하는지를 스트림 공급 수단(150, 160)이 알고 있어야 하기 때문이다.

상기 내부 스트림 공급 수단(150)은 전술한 바와 같이 파일 시스템 영역(200)내에서 외부 스트림 공급 수단(160)에 특정 컨텐츠 데이터를 요청(S3)하고 이 요청에 대한 응답으로 전송(S6)받은 데이터를 다시 상기 필터링 수단(120)을 거쳐 특정 실행 프로그램(130)으로 전송(S7)하여 실행 가능토록 하는 기능을 수행한다. 따라서 내부 스트림 공급 수단(150)은 어느 외부 스트림 공급 수단과 통신해야 하는 지와, 요청하는 컨텐츠 데이터에 관한 정보를 사전에 알고 있어야 하며, 이것들은 전술한 바와 같이 제어기(110)에 의해 단계(S1') 등에서 사전에 제공된다.

본 발명에서 저장 장치(170)에 저장된 컨텐츠 데이터는 임의의 특정 DRM에 의해 암호화된 데이터일 수 있다. DRM 암호화/복호화는 당업계의 통상의 기술을 가진 전문가들에게 잘 알려져 있는 기술로서, 각각의 DRM 방식마다 고유의 방식으로 암호화 및 복호화를 수행하는 특징을 가진다. 따라서, 어떤 DRM 방식에 의해 암호화된 데이터는 이 방식의 DRM 복호화기 외에 다른 DRM 복호화기로는 복호화를 할 수 없다. 도 1의 컨텐츠 데이터 파일인 C.avi가 임의의 특정 DRM에 의해서 암호화된 것이라면, 이것을 복호화하는 것도 이 특정 DRM의 복호화기에 의해서만 가능하다. 본 발명에서 외부 스트림 공급 수단(160)은 이러한 DRM 복호화기의 역할 및 데이터 중계 역할을 수행할 수 있는데, 이 경우 제어기(110)는 사전에 선택된 컨텐츠 데이터의 암호화 방식에 대응하는 복호화 기능을 가진 스트림 공급 수단을 외부 스트림 공급 수단으로 선정해서 내부 스트림 공급 수단(150)에 통보해 주어야 한다.

도 1에서 내부 스트림 공급 수단에 의해 데이터 전송 요청을 받은 외부 스트림 공급 수단 B.exe(160)는 내부 스트림 공급 수단(150)으로부터 제공받은 컨텐츠 데이터에 관한 정보를 이용하여 해당 컨텐츠 데이터를 저장한 영역인 특정 저장 장치(170)을 찾아내고 이로부터 데이터를 전송 받는다.

외부 스트림 공급 수단(160)은 전송받은 컨텐츠 데이터를 내부 스트림 공급 수단(150)으로 전송하는데, 이 데이터가 암호화된 것이라면 전술한 방식으로 복호화하여 전달한다. 데이터를 전송받은 내부 스트림 공급 수단(150)은 전송받은 데이터를 어느 실행 프로그램이 호출한 데이터인지를 식별한 후, 필터링 수단(120)을 통하여 이 컨텐츠 데이터를 실행 프로그램(130)에 전송하고, 실행 프로그램(130)은 전송받은 일정량의 스트림 데이터를 실행함으로써 컨텐츠 데이터의 호출 및 실행이 완료된다.

이 컨텐츠 데이터는 컨텐츠 데이터 파일 전체의 일부분인 스트림 데이터이고, 실행 프로그램(130) 또는 내부 스트림 공급 수단(150)이 한번에 요청할 데이터 양을 결정해서 매번마다 전술한 방식으로 데이터를 요청해서 실행 프로그램에서 실행되도록 할 수 있다.

도 1에서, 만약 등록되지 않은 실행 프로그램인 D.exe(140)가 컨텐츠 데이터를 실행하고자 데이터 파일을 호출하는 경우(S8)에, 이것은 필터링 수단(120)에 사전에 등록되지 않은 실행 프로그램이므로, 호출(S8)은 필터링 수단에 의해 유효하지 않은 호출이 되어 에러 메시지 등이 응답되고 데이터는 실행되지 않는다.

도 1의 시스템은 암호화가 풀린 상태의 데이터를 특정 필터링 수단이 제어하는 파일 시스템 영역에 보관하고, 특정 실행 프로그램만이 이를 실행할 수 있도록 함으로써 사용자의 데이터 무단 복제 및 배포를 방지하는 동시에 이를 스트림

방식으로 실행되도록 한 것에 특징이 있다. 한 예로 상기 특정 실행 프로그램이 읽기 외에 복제나 데이터 전송 및 배포를 할 수 없는 것이라면 이러한 무단 복제가 방지될 수 있는 것이다. 사용자는 이 경우 저장이나 데이터 전송을 할 수 있는 다른 실행 프로그램으로 실행 명령을 내릴 수 있지만, 이 다른 실행 프로그램은 제어기(110)에 의해 등록되지 않은 실행 프로그램이므로 이 명령은 실행되지 않게 된다.

비록 지금까지 설명한 경우는 내부 스트림 공급 수단과 외부 스트림 공급 수단을 구분하여 기술하였지만, 반드시 양자가 분리되어 있는 것은 아니다. 즉, 하나의 스트림 공급 수단만으로도 동일한 작동을 할 수 있는데, 이것은 스트림 공급 수단의 기능이 실행 프로그램으로부터의 유효한 실행 요청을 받아 목표로 하는 컨텐츠 데이터를 불러오고 이를 실행 프로그램에 공급하는 것이므로, 이러한 기능만 수행할 수 있으면 본 발명의 스트림 공급 수단으로 적용될 수 있기 때문이다. 다만, 도 1의 실시예에서 이를 구분한 것은 전술한 복호화 기능이나 이하에서 설명되는 라이브러리 형태의 공급 수단, 또는 네트워크로 파일 시스템과 외부 스트림 공급 수단이 연결된 경우 등에는 두 스트림 공급 수단이 물리적, 기능적으로 구분되어야 하기 때문이다. 참고로 도 2에는 내부 스트림 공급 수단만이 제공된 경우를 보여주고 있는데, 내부 스트림 공급 수단(150)은 제어기(110)로부터 전달받은 컨텐츠 데이터 정보를 이용하여 저장장치(170)에 직접 데이터를 요청하고(S3') 전달받아(S5') 실행 프로그램(130)에 제공한다(S7).

도 3은 스트림 공급 수단으로서 내부 스트림 공급 수단(150)만이 존재하면서, 동시에 저장 장치(170)에 저장된 컨텐츠 데이터(C.avi)가 암호화된 데이터일 경우, 파일 시스템 내부의 복호화 수단(180)이 이를 복호화해서 실행 프로그램(130)으로 전송하는 경우를 도시하고 있다. 즉, 내부 스트림 공급 수단(150)이 암호화된 상태인 컨텐츠 데이터를 전달하면(S6') 이 데이터는 실행 프로그램으로 전달되기 전에 복호화되어 전달된다(S7). 복호화 수단(180)의 위치는 본 실시예에서 도시된 것처럼 반드시 실행 프로그램의 전단계에 존재하여 실행 프로그램으로는 복호화된 데이터를 전달할 수 있으면 되므로, 그 위치는 저장 장치 및 실행 프로그램 사이의 어느 곳이라도 무방하다.

도 4는 외부 스트림 공급 수단이나 컨텐츠 데이터 저장 장치의 위치가 클라이언트 시스템을 벗어나 위치하고, 네트워크를 통해 클라이언트 시스템과 연결된 경우의 또 다른 실시예를 보여주고 있다.

도 4에서, 만약 외부 스트림 공급 수단은 www.k.net/B.exe로, 데이터가 존재하는 네트워크 상의 위치는 www.e.net/f.avi(270)로 제어기(110)에 의해 파일 시스템 영역(200)에 입력된다면, 내부 스트림 공급 수단(150)은 이러한 정보를 이용하여 www.k.net에 존재하는 외부 스트림 공급 수단 B.exe를(260)을 활성화시키고, www.e.net로부터 f.avi이라는 컨텐츠 데이터 파일을 가져오라는 명령을 내리게 된다. 나머지 도 1과 동일한 도면 부호가 붙은 모듈들의 기능은 도 1의 실시예와 동일하거나 유사하다.

도 4에서는 데이터의 위치 및 외부 스트림 공급 수단 모두가 클라이언트 시스템 외부에 존재하는 경우를 상정하였지만, 둘 중 어느 하나만이라도 클라이언트 시스템의 외부에 존재하는 경우도 가능하다. 또한, 예시를 위하여 인터넷 URL로 클라이언트 시스템의 외부를 나타내고 있으나, 인트라넷 및 주변 저장 장치를 포함한 기타 네트워크도 모두 이 설명에 포함되는 실시예들이다.

도 5는 본 발명의 또 다른 실시예를 보여주고 있다. 도 1 및 도 4의 실시예의 경우에는, 파일 시스템 영역(200)내에 컨텐츠 데이터에 관한 정보를 공급하고, 이를 내부 스트림 공급 수단(150)이 다시 외부 스트림 공급 수단(160)에 통지하는 간접적인 방식을 취하였으나, 도 5의 경우는 제어기(110)가 컨텐츠 데이터에 관한 정보를 외부 스트림 공급 수단(160)에 직접 통지(S1 ")하는 방식이 전술한 실시예와는 다른 점이다. 이 정보를 받은 외부 스트림 공급 수단(160)은 스스로 컨텐츠 데이터를 찾아서 내부 스트림 공급 수단에 제공한다. 이 때의 외부 스트림 공급 수단은 자신의 실행을 스스로 제어할 수 있는 실행 프로그램이어야 한다.

외부 스트림 공급 수단의 종류에는 상기 도 5의 B.exe(160)처럼 독립적으로 다른 모듈로부터 실행을 의뢰받아 수행하는 프로그램도 가능하지만, 내부 스트림 공급 수단(150)의 제어를 받아 수동적으로 기능하는 모듈도 가능하다. 가령, 라이브러리 형태의 프로그램이 대표적인 경우인데, 이 경우 라이브러리인 외부 스트림 공급 수단의 실행 및 제어는 내부 스트림 공급 수단(150)이 관리하게 된다. 라이브러리란 실행 프로그램의 일부 기능을 수행하는 모듈로서 가령, 읽기나 쓰기 등을 실행 프로그램 본체가 직접 수행하는 것이 아니라 외부의 라이브러리에게 실행시키고 이를 본체가 제어하는 것으로서, 원도우 시스템에서는 DLL(동적 라이브러리)가 일반적이며 유닉스 시스템에서는 두 개 이상의 실행 프로그램이 동일한 기능의 모듈을 공유하게 하는 공유 라이브러리(shared library)가 있다. 도 6에서는 외부 DLL인 B.dll(160')을 이용하여 컨텐츠 데이터를 호출하여 불러오는 경우를 도시하고 있다. 외부 스트림 공급 수단이 라이브러리인 경우, 컨텐츠 데이터에 관한 정보는 내부 스트림 공급 수단에 우선 제공되어야 하며, 이 때의 외부 스트림 공급 수단은 단순히 데이터의 입력 및 전송을 수행하는 모듈이고, 나머지 데이터 처리는 반드시 프로그램 본체인 내부 스트림 공급 수단이 수행하게 된다. 이에 반해 도 5의 모듈(160)은 독립적인 프로그램이다. 본 발명에서는 도 6의 모듈(160')같은 경우를 라이브러리로 칭하지만, DLL이나 공유 라이브러리 외에 동일한 구성을 가진 다른 모듈들도 모두 이에 포함되는 개념이다.

도 7은 본 발명의 또 다른 실시예에 대한 것이다. 도 7은 파일 시스템 내부(200)에서 내부 스트림 공급 수단(150)과 실행 프로그램(130) 사이에 버퍼 메모리(400)가 추가된 경우를 보여주는 것으로서, 그 외 다른 모듈들은 도 1과 동일하므로 생략하였다.

도 7에서는 외부 스트림 공급 수단(도시되지 않음)으로부터 내부 스트림 공급 수단(150)으로 스트림 데이터가 전송되면(S6), 이 데이터는 내부 스트림 전송 수단에 의해 버퍼 메모리에 저장된다(S42). 저장된 데이터는 유효한 실행 프로그램(130)의 실행 호출에 대한 응답으로 실행 프로그램으로 전송(S7')되어 실행되며, 그 사이에 후속 스트림 데이터들이 계속 동일한 과정을 거쳐 버퍼 메모리(400)에 공급된다. 이 실시예의 장점은 버퍼 메모리라는 임시 메모리 풀(pool)내에 실행 프로그램(130)의 실행 호출에 대해 언제든지 전송할 준비가 된 데이터를 충분히 저장하므로써, 실행시 전송 속도의 문제로 인한 데이터 실행의 끊어짐 등에 대비할 수 있다는 점이다.

도 7에서, 실행 프로그램의 호출(S2')에 의해 먼저 버퍼 메모리(400)를 검색하여 데이터의 유무를 판단하고, 데이터가 없으면 내부 스트림 전송 수단(150)에 통보하여 데이터의 전송을 요청한다(S41). 그 다음, 이 전송 요청(S41)을 받은 내부 스트림 공급 수단(150)은 외부 스트림 공급 수단과 통신하여(S3) 데이터를 공급받아(S6) 버퍼 메모리의 빈 공간만큼 데이터를 채운다. 버퍼 메모리(400) 내의 데이터 유무 판단은 실행 프로그램(130)이 수행할 수도 있고, 버퍼 메모리 자신이 수행할 수도 있다.

또한, 실행 프로그램의 데이터 요청(S2')과 버퍼 메모리에 대한 내부 스트림 공급 수단(150)의 데이터 전송(S42)은 서로 독립적으로 작동할 수 있다. 즉, 처음 컨텐츠 데이터 요청 명령을 전달받은 내부 스트림 공급 수단(150)은 이 후부터는 버퍼 메모리(400)가 비어있는 것을 감지하면, 실행 프로그램(130)의 후속 스트림 데이터 요청 명령의 유무를 묻지 않고 무조건적으로 이를 채우기 위해 외부로 데이터를 요청하여 버퍼 메모리를 채워 넣는 방식이다.

도 8은 본 발명의 또 다른 실시예를 나타내는 것으로, 여기서는 버퍼 메모리(400)를 전후하여 암호화 수단(510) 및 복호화 수단(520)을 추가로 구비하고 있다. 이 경우, 내부 스트림 공급 수단(150)에 의해 실행 프로그램으로 제공되는 암호화되지 않은 컨텐츠 데이터는 암호화 수단(510)을 거치면서(S43), 암호화된 상태로 버퍼 메모리(400)내에 임시 저장된다. 그 다음 실행 프로그램으로 전달되는 단계(S44)에서 복호화 수단(520)을 거쳐 암호화가 풀린 후 실행 프로그램으로 전달된다. 이러한 암호화 및 복호화를 수행하는 이유는 버퍼 메모리에 임시로 저장되는 데이터를 보호하기 위

해서이다. 즉, 도 8의 구성에서는 버퍼 메모리에 저장되는 데이터가 암호화된 것이므로, 이 데이터를 버퍼 메모리로부터 사용자가 어떤 방법으로든 추출해낸다 하더라도 복호화 수단이 없는 이상 무단으로 사용하지 못하기 때문이다. 상기 암호화는 당업자에게 잘 알려진 1회용 암호화 키를 사용하여 매번 복호화 키가 변화되도록 할 수 있다.

본 발명의 도 1 내지 도 8까지 설명한 실시예들은 서로 조합되어 구현될 수 있다. 가령, 도 2의 구성에 도 7의 버퍼링 수단을 부가하거나, 도 1의 수단에 도 8의 수단을 부가하는 방식 등 다양한 조합이 가능한데, 이러한 조합들 역시 본 발명에서 보여주고자 하는 실시예들임을 밝힌다.

발명의 효과

본 발명을 이용하면, 컨텐츠 데이터를 스트림 방식으로 실행시킬 때, 암호가 풀린 데이터를 사용자가 해킹하여 무단으로 복제하거나 배포하는 등의 행위를 원천적으로 방지할 수 있다.

또한, 본 발명에서는 기존의 DRM 방식처럼 실행 프로그램과 복호화 수단이 서로 매칭되어 존재할 필요가 없어지므로, 시스템에 가해지는 로드 등을 효과적으로 감소시키면서, 동시에 기존 DRM 방식의 장점을 그대로 이용할 수 있게 된다.

이러한 본 발명의 장점을 이용하면, 컨텐츠 데이터 공급자의 리스크를 획기적으로 감소시킬 수 있으므로, 컨텐츠 데이터의 원할한 사회적 이용을 도모할 수 있다.

본 발명의 스트림 방식으로 실행되는 데이터란 일반적인 스트림 데이터를 의미하는 것으로, 파일 전체 데이터 중 일부 데이터가 실행되면서, 동시 또는 순차적으로 그 다음 데이터의 입력이 실행되는 경우를 말하며, 선행 데이터와 그 다음 데이터의 실행을 위한 데이터 호출이 서로 동시에 또는 순차적으로 진행되는 모든 경우를 포함한다. 또한, 본 발명에서 컨텐츠 데이터란 광범위하게는 문서 파일, 그래픽 파일, 오디오 파일 및 동영상 파일 등을 포함하여 실행 프로그램에 대응하는 모든 자료 데이터를 포함하는 개념이다.

본 발명에서 모듈이란 전술한 본 발명의 여러 기능을 각각 수행하는 가장 기본적인 기능 단위 또는 다수 기능을 함께 수행하는 복합 기능 단위를 모두 포함하는 개념이며, 또한 각 모듈간 데이터 통신은 통신해야 할 모듈들끼리 수동적인 역할 및 능동적인 역할, 가령 데이터의 요청이나 전송을 필요에 따라 서로 바꾸어 수행하도록 할 수도 있다.

본 발명에서 데이터 통신이란 관련 모듈간의 데이터 요청 및 데이터 전송을 모두 포함하는 개념이다.

당업자라면 본 발명의 기술적 사상의 범주 내에서 상기 실시예에 대한 다양한 변형예가 가능함을 쉽게 인식할 수 있을 것이며, 본 발명이 청구하고자 하는 권리범위는 상기 실시예에 국한되지 않고, 오로지 아래에 기술되는 청구범위에 의해 정의된다.

(57) 청구의 범위

청구항 1.

스트림 방식으로 실행되는 스트림 데이터를 보호하기 위한 시스템에 있어서,

실행하고자 요청된 스트림 데이터의 정보 및 이 스트림 데이터를 실행할 수 있는 실행 프로그램의 식별 정보를 제공하는 제어 수단과,

상기 제공된 실행 프로그램의 식별 정보를 저장하고, 소정의 실행 프로그램이 상기 스트림 데이터를 실행하고자 요청하는 경우에 상기 소정의 실행 프로그램의 식별 정보가 저장되었는지를 판단하고, 상기 소정의 실행 프로그램의 식별 정보가 저장되었다고 판단되면 상기 실행 요청을 유효한 것으로서 통과시키는 필터링 수단과,

상기 필터링 수단을 통과한 스트림 데이터 요청을 입력받으면, 상기 제공된 스트림 데이터의 정보를 바탕으로 스트림 데이터를 요청하고, 요청된 스트림 데이터를 공급받으면 상기 스트림 데이터를 요청한 실행 프로그램에 제공하는 스트림 데이터 공급 수단

을 포함하는 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 2.

제1항에 있어서, 상기 스트림 데이터를 저장하고 있으면서, 상기 스트림 공급 수단으로부터의 요청에 응답하여 저장된 스트림 데이터를 상기 스트림 공급 수단으로 제공하는 스트림 데이터 저장 수단을 더 포함하는 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 3.

제1항에 있어서, 상기 요청된 스트림 데이터가 암호화된 데이터일 경우, 이를 복호화하여 상기 스트림 데이터 공급 수단으로 제공하는 복호화 수단을 더 포함하는 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 4.

제2항에 있어서, 상기 스트림 데이터 공급 수단은, 반드시 상기 필터링 수단을 통해서 실행 프로그램과의 데이터 통신을 수행하는 제1 스트림 공급 수단과, 상기 스트림 데이터 저장 수단으로부터 스트림 데이터를 공급받아 상기 필터링 수단을 통하지 않고 상기 제1 스트림 공급 수단과 데이터 통신을 수행하는 제2 스트림 공급 수단을 포함하는 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 5.

제4항에 있어서, 상기 제2 스트림 공급 수단은 상기 제1 스트림 공급 수단의 라이브러리인 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 6.

제4항에 있어서, 상기 제2 스트림 공급 수단은 독립적으로 실행될 수 있는 모듈인 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 7.

제4항에 있어서, 상기 제2 스트림 공급 수단은 상기 제1 스트림 공급 수단과 서로 원거리에 위치하면서 네트워크로 연결된 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 8.

제6항에 있어서, 상기 실행하고자 요청된 스트림 데이터의 정보는 상기 제어 수단에 의해 특히 상기 제2 스트림 공급 수단에 직접 제공되는 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 9.

제4항 내지 제8항 중 어느 한 항에 있어서, 상기 제2 스트림 공급 수단은 복호화 수단인 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 10.

제2항에 있어서, 상기 스트림 데이터 저장 수단은 상기 스트림 공급 수단과 서로 원거리에 위치하면서 네트워크로 연결되는 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 11.

제1항에 있어서, 상기 실행 프로그램과 상기 스트림 데이터 공급 수단 사이에 버퍼링 수단을 추가로 포함하고, 상기 스트림 데이터 공급 수단이 요청된 스트림 데이터를 공급받으면 상기 버퍼링 수단을 통해서 상기 실행 프로그램으로 스트림 데이터를 제공하는 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 12.

제11항에 있어서, 상기 스트림 데이터 공급 수단과 버퍼링 수단 사이에는 암호화 수단을, 상기 버퍼링 수단과 상기 실행 프로그램 사이에는 상기 암호화 수단에 대응하는 복호화 수단을 추가로 포함하는 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 13.

제12항에 있어서, 상기 암호화 수단 및 복호화 수단은 1회용 암호화 키 방식으로 암호화 및 복호화를 수행하는 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 14.

제1항에 있어서, 상기 요청된 스트림 데이터가 암호화된 데이터일 경우, 이를 복호화하여 상기 실행 프로그램으로 제공하는 복호화 수단을 더 포함하는 것을 특징으로 하는 스트림 데이터 보호 시스템.

청구항 15.

스트림 방식으로 실행되는 스트림 데이터를 보호하는 방법에 있어서,

실행하고자 요청된 스트림 데이터의 정보 및 이 스트림 데이터를 실행할 수 있는 실행 프로그램의 식별 정보를 제공하는 단계와,

상기 제공된 실행 프로그램의 식별 정보를 필터링 수단에 저장하는 단계와,

소정의 실행 프로그램이 상기 스트림 데이터를 실행하고자 요청하는 경우에 상기 소정의 실행 프로그램의 식별 정보가 상기 필터링 수단에 저장되었는지를 판단하고, 상기 소정의 실행 프로그램의 식별 정보가 저장되었다고 판단되면 상기 실행 요청을 유효한 것으로서 스트림 데이터 공급 수단으로 전송하는 단계와,

상기 전송된 스트림 데이터 요청을 입력받은 상기 스트림 데이터 공급 수단이 상기 제공된 스트림 데이터의 정보를 바탕으로 스트림 데이터를 요청하는 단계와,

상기 스트림 데이터 공급 수단이 요청된 스트림 데이터를 공급받으면 상기 스트림 데이터를 요청한 실행 프로그램으로 이 스트림 데이터를 제공하는 단계

를 포함하는 것을 특징으로 하는 스트림 데이터 보호 방법.

청구항 16.

제15항에 있어서, 상기 요청된 스트림 데이터가 암호화된 데이터일 경우, 이를 복호화하여 상기 소정의 스트림 데이터 공급 수단으로 제공하는 복호화 단계를 더 포함하는 것을 특징으로 하는 스트림 데이터 보호 방법.

청구항 17.

제15항에 있어서, 상기 소정의 스트림 데이터 공급 수단이 요청된 스트림 데이터를 공급받아서 상기 실행 프로그램으로 스트림 데이터를 제공하는 단계 이전에 이 스트림 데이터를 버퍼링하는 단계를 더 포함하는 것을 특징으로 하는 스트림 데이터 보호 방법.

청구항 18.

제17항에 있어서, 상기 버퍼링 단계 이전에 상기 스트림 데이터를 암호화하는 단계와, 상기 버퍼링 단계 이후에 상기 암호화된 스트림 데이터를 복호화하는 단계를 추가로 포함하는 것을 특징으로 하는 스트림 데이터 보호 방법.

청구항 19.

제15항에 있어서, 상기 스트림 데이터가 암호화된 데이터일 경우 상기 스트림 데이터를 요청한 실행 프로그램으로 스트림 데이터를 제공하는 단계 이전에 상기 스트림 데이터를 복호화하는 단계를 추가로 포함하는 것을 특징으로 하는 스트림 데이터 보호 방법.

청구항 20.

스트림 방식으로 실행되는 스트림 데이터를 보호하기 위한 컴퓨터 프로그램의 저장 매체에 있어서,

실행하고자 요청된 스트림 데이터의 정보 및 이 스트림 데이터를 실행할 수 있는 실행 프로그램의 식별 정보를 제공하는 제어 수단과,

상기 제공된 실행 프로그램의 식별 정보를 저장하고, 소정의 실행 프로그램이 상기 스트림 데이터를 실행하고자 요청하는 경우에 상기 소정의 실행 프로그램의 식별 정보가 상기 접근 제어 수단에 저장되었는지를 판단하고, 상기 소정의 실행 프로그램의 식별 정보가 저장되었다고 판단되면 상기 실행 요청을 유효한 것으로서 통과시키는 필터링 수단과,

상기 필터링 수단을 통과한 스트림 데이터 요청을 입력받으면, 상기 제공된 스트림 데이터의 정보를 바탕으로 스트림 데이터를 요청하고, 요청된 스트림 데이터를 공급받으면 상기 스트림 데이터를 요청한 실행 프로그램에 제공하는 스트림 데이터 공급 수단

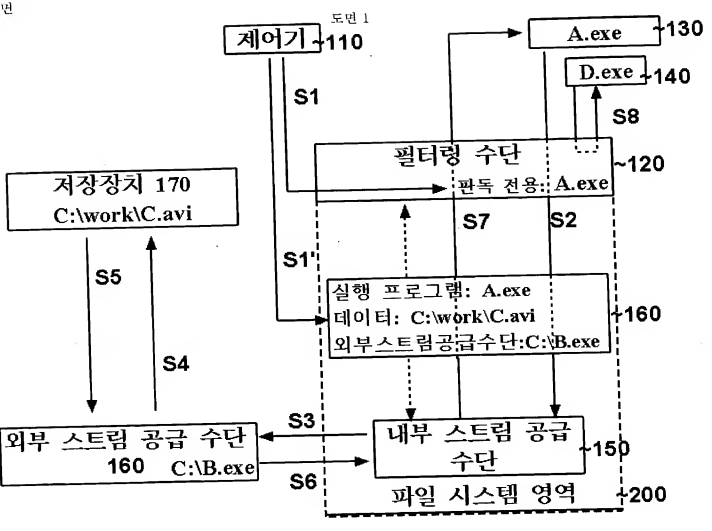
을 포함하는 것을 특징으로 하는 스트림 데이터 보호를 위한 컴퓨터 프로그램의 저장 매체.

청구항 21.

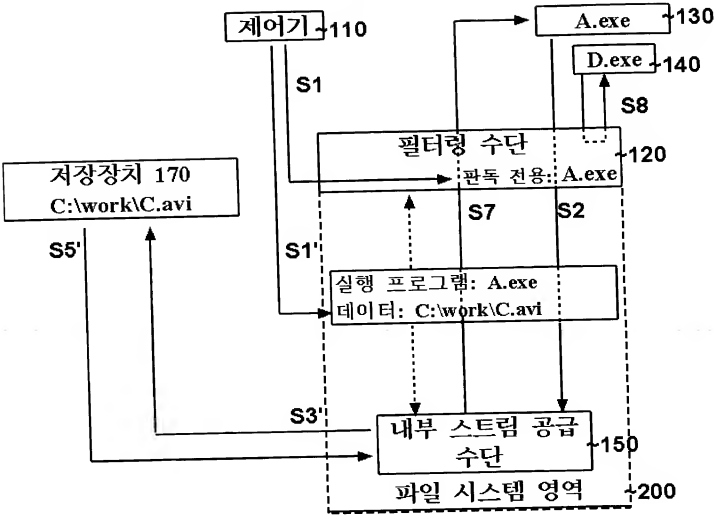
제20항에 있어서, 상기 실행 프로그램과 상기 스트림 데이터 공급 수단 사이에 위치하면서, 상기 스트림 데이터 공급 수단이 요청된 스트림 데이터를 공급받아 상기 실행 프로그램으로 스트림 데이터를 제공하기 전에 상기 스트림 데이터를 버퍼링 하는 버퍼링 수단을 추가로 포함하는 것을 특징으로 하는 스트림 데이터 보호를 위한 컴퓨터 프로그램의 저장 매체.

도면

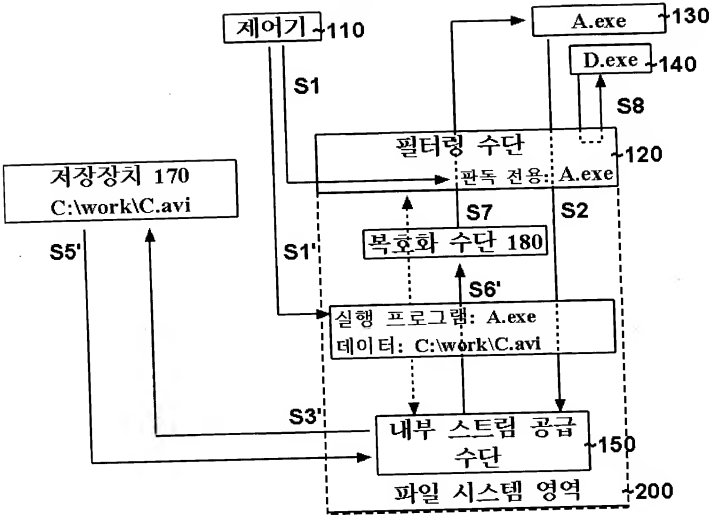
도면 1


제어기
110
A.exe
130
D.exe
140
S1
S8
필터링 수단
120
판독 전용: A.exe
저장장치 170
C:\work\C.avi
S7
S2
S1'
S5
실행 프로그램: A.exe
데이터: C:\work\C.avi
외부스트림공급수단:C:\B.exe
160
S4
S3
외부 스트림 공급 수단
160 C:\B.exe
내부 스트림 공급
수단
150
S6
파일 시스템 영역
200

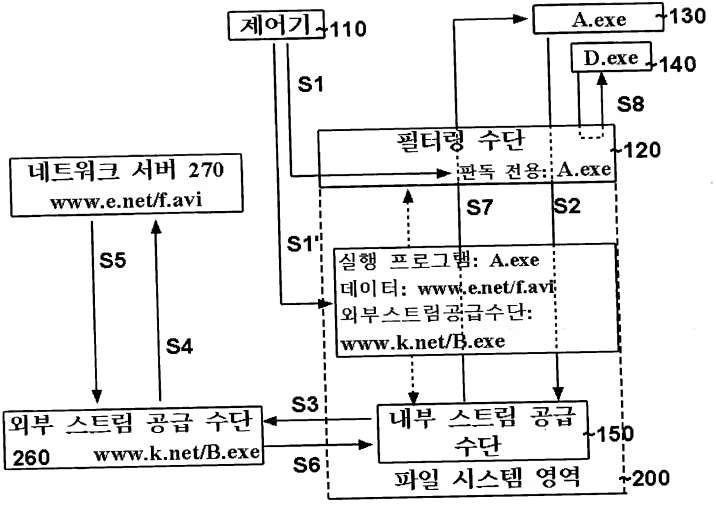
도면 2


제어기
110
A.exe
130
D.exe
140
S1
S8
필터링 수단
120
판독 전용
A.exe
저장장치 170
C:\work\C.avi
S7
S2
S5'
S1'
실행 프로그램: A.exe
데이터: C:\work\C.avi
S3'
내부 스트림 공급 수단
150
파일 시스템 영역
200

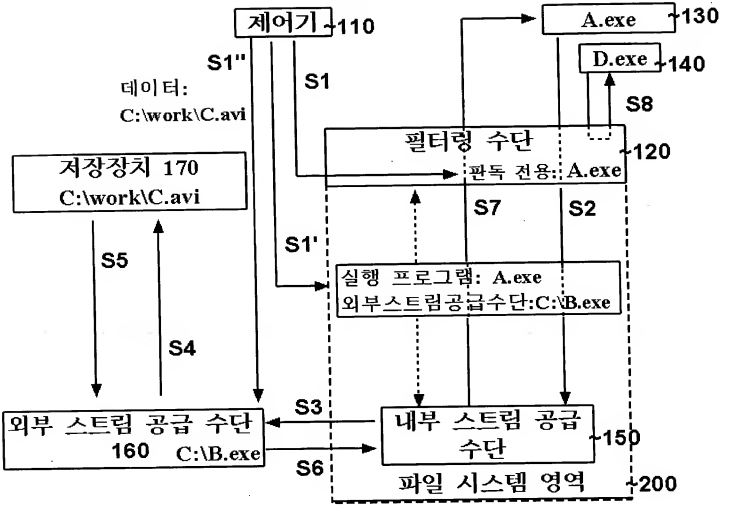
도면 3


제어기
110
A.exe
130
D.exe
140
S1
S8
필터링 수단
120
판독 전용: A.exe
저장장치 170
C:\work\C.avi
S7
S2
S5'
S1'
복호화 수단 180
S6'
실행 프로그램: A.exe
데이터: C:\work\C.avi
S3'
내부 스트림 공급 수단
150
파일 시스템 영역
200

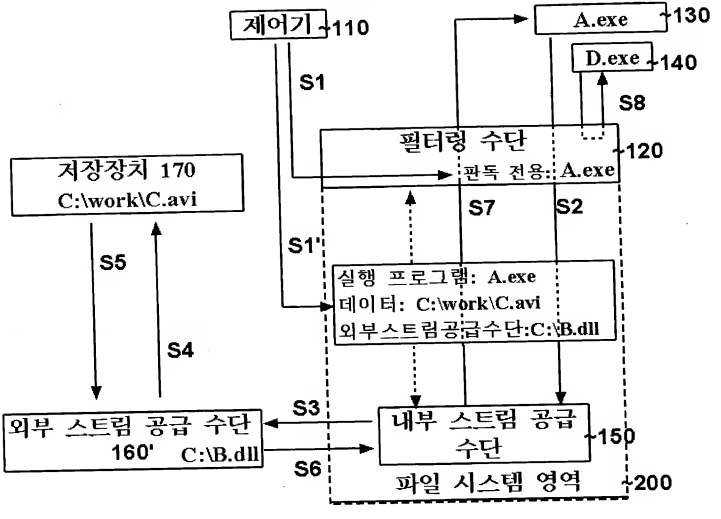
도면 4


제어기
110
A.exe
130
D.exe
140
S1
S8
필터링 수단
120
판독 전용: A.exe
네트워크 서버 270
www.e.net/f.avi
S7
S2
S1'
S5
실행 프로그램: A.exe
데이터: www.e.net/f.avi
외부스트림공급수단:
www.k.net/B.exe
S4
S3
외부 스트림 공급 수단
260
www.k.net/B.exe
내부 스트림 공급
수단
150
S6
파일 시스템 영역
200

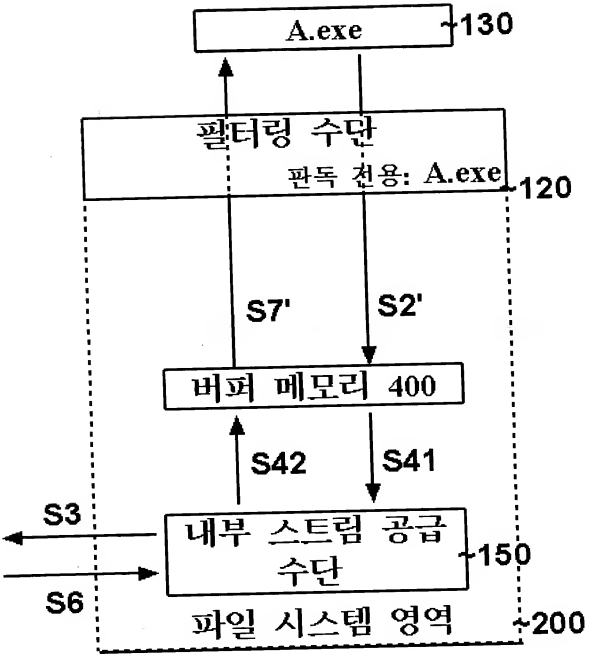
도면 5


제어기
110
A.exe
130
D.exe
140
S1"
S1
데이터:
C:\work\C.avi
S8
필터링 수단
120
판독 전용: A.exe
저장장치 170
C:\work\C.avi
S7
S2
S1'
S5
실행 프로그램: A.exe
외부스트림공급수단:C:\B.exe
S4
S3
외부 스트림 공급 수단
160
C:\B.exe
내부 스트림 공급
수단
150
S6
파일 시스템 영역
200

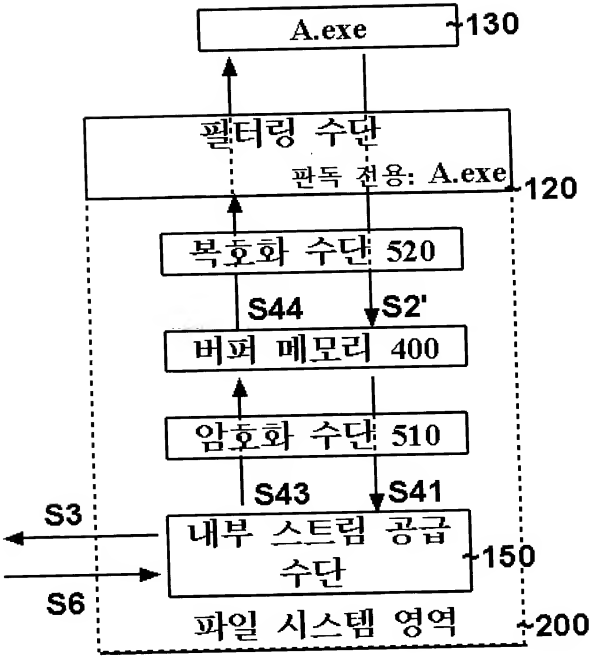
도면 6


제어기
110
A.exe
130
D.exe
140
S1
S8
필터링 수단
120
판독 전용: A.exe
저장장치 170
C:\work\C.avi
S7
S2
S1'
S5
실행 프로그램: A.exe
데이터: C:\work\C.avi
외부스트림공급수단:C:\B.dll
S4
S3
외부 스트림 공급 수단
160'
C:\B.dll
내부 스트림 공급
수단
150
S6
파일 시스템 영역
200

도면 7


A.exe
130
필터링 수단
판독 전용: A.exe
120
S7'
S2'
버퍼 메모리 400
S42
S41
S3
내부 스트림 공급 수단
150
S6
파일 시스템 영역
200

도면 8


A.exe
130
필터링 수단
판독 전용: A.exe
120
복호화 수단 520
S44
S2'
버퍼 메모리 400
암호화 수단 510
S43
S41
S3
내부 스트림 공급 수단
150
S6
파일 시스템 영역
200